N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 13

Aufgabe 49 Seien $M|L|K$ Körpererweiterungen. Man zeige folgendes.

(1) Seien M und L algebraische Abschlüsse von K. Dann ist $M = L$.

(2) Sei M ein algebraischer Abschluss von K.
Dann ist M auch ein algebraischer Abschluss von L.

Lösung zu Aufgabe 49:

(1) Es genügt, $M \subseteq L$ zu zeigen.

Da M algebraischer Abschluss von K ist, ist jedes Element $y \in M$ algebraisch über K. D.h. für $y \in M$ gibt es ein normiertes Polynom $f(X) \in K[X]$ mit $f(y) = 0$.

Als algebraischer Abschluss von K ist L insbesondere algebraisch abgeschlossen. D.h. $f(X) \in K[X] \subseteq L[X]$ zerfällt in $L[X]$ in normierte Faktoren von Grad 1. Also ist $y \in L$.

(2) Als algebraischer Abschluss von K ist M insbesondere algebraisch abgeschlossen.

Sei $y \in M$. Dann ist y algebraisch über K, d.h. es gibt ein normiertes Polynom $f(X) \in K[X]$ mit $f(y) = 0$. Da $K(X) \subseteq L[X]$ ist, ist $y \in M$ ist algebraisch über L.

Somit ist M auch algebraischer Abschluss von L.

Aufgabe 50 Man zeige oder widerlege.

(1) $\mathbb{F}_5$ ist algebraisch abgeschlossen.

(2) Sei $n \in \mathbb{Z}_{\geqslant 1}$ und d ein Teiler von n. Sei $K \subseteq \mathbb{F}_{p^n}$ ein Teilkörper mit $|K| = p^d$. Dann ist $K = \{x \in \mathbb{F}_{p^n} : x^{p^d} = x\}$.

(3) Sei $n \in \mathbb{Z}_{\geqslant 1}$. Es hat $\mathbb{F}_{p^n}$ einen Teilkörper mit d Elementen für jeden Teiler $d \neq 1$ von p^n.

(4) Es hat $\mathbb{F}_{64}$ genau 4 Teilkörper.

Lösung zu Aufgabe 50:

(1) Falsch. Sei $f(X) := \left(\prod_{a \in \mathbb{F}_5} (X - a)\right) + 1 \in \mathbb{F}_5[X]$.

Nach Konstruktion gilt $f(a) = 1$ für alle $a \in \mathbb{F}_5$, also hat $f(X)$ keine Nullstelle in $\mathbb{F}_5$.

Somit ist $\mathbb{F}_5$ nicht algebraisch abgeschlossen.

(2) Richtig. Es ist $\mathrm{U}(K) = K^\times \simeq \mathrm{C}_{p^d-1}$, daher gilt für alle $x \in K^\times$, dass $x^{p^d-1} = 1$ ist. Somit gilt für $x \in K$, dass $x^{p^d} = x$ ist, auch für $x = 0$. Also ist $K \subseteq \{x \in \mathbb{F}_{p^n} : x^{p^d} = x\}$. Das Polynom $X^{p^d} - X$ hat höchstens p^d Nullstellen in $\mathbb{F}_{p^n}$, und da $|K| = p^d$ ist, folgt $K = \{x \in \mathbb{F}_{p^n} : x^{p^d} = x\}$.

(3) Falsch. Es ist $[\mathbb{F}_8 : \mathbb{F}_2] = 3$ und 4 ein Teiler von 8.

Annahme, es gibt einen Teilkörper Z mit $|Z| = 4$, dann ist $\mathbb{F}_2 \subseteq Z$ und $[Z : \mathbb{F}_2] = 2$. Es folgt, $3 = [\mathbb{F}_8 : \mathbb{F}_2] = [\mathbb{F}_8 : Z][Z : \mathbb{F}_2] = [\mathbb{F}_8 : Z] \cdot 2$. *Widerspruch.*

(4) Richtig.

Wir zeigen, dass es für jeden Teiler d von n einen Teilkörper von $\mathbb{F}_{p^n}$ mit p^d Elementen gibt.

Es ist $K = K_d := \{x \in \mathbb{F}_{p^n} : x^{p^d} = x\}$ ein Teilkörper von $\mathbb{F}_{p^n}$ mit p^d Elementen:

Teilkörper: Es ist $1 \in K$. Seien $x, y \in K$. Dann ist $(x+y)^{p^d} = x^{p^d} + y^{p^d} = x + y$ und $(x \cdot y)^{p^d} = x^{p^d} \cdot y^{p^d} = x \cdot y$, d.h. $x + y, x \cdot y \in K$.

Es ist $1^{p^d} = (x^{-1} \cdot x)^{p^d} = (x^{-1})^{p^d} \cdot x^{p^d}$, d.h. $(x^{-1})^{p^d} = x^{-1}$, d.h. $x^{-1} \in K$.

K hat p^d Elemente. Es ist $|K| \leqslant p^d$. Es genügt zu zeigen, dass es $p^d - 1$ Elemente x in $\mathbb{F}_{p^n}^\times$ gibt, die die Gleichung $x^{p^d-1} = 1$ erfüllen. Sei c ein Erzeuger von $\mathbb{F}_{p^n}^\times$. Es hat c die Ordnung $p^n - 1$.

Da d ein Teiler von n ist, gibt es ein $k \in \mathbb{Z}$ mit $n = k \cdot d$. Es ist $p^d - 1$ ein Teiler von $p^n - 1$, da $p^n - 1 = (p^d)^k - 1 = (p^d - 1)\left(\sum_{i \in [0,k-1]} p^{id}\right)$ ist.

Also hat $a := c^{\frac{(p^n-1)}{(p^d-1)}}$ Ordnung $|\langle a \rangle| = p^d - 1$ und alle Elemente $x \in \langle a \rangle$ erfüllen $x^{p^d-1} = 1$.

> *Alternativ:* Das Polynom $X^{p^n} - X$ zerfällt in $\mathbb{F}_{p^n}$ in verschiedene normierte Faktoren von Grad 1, da jedes $x \in \mathbb{F}_{p^n}$ eine Nullstelle ist. Es ist $X^{p^n} - X = (X^{p^d} - X) \cdot (\sum_{k \in \left[0, \frac{p^n-1}{p^d-1}\right]} X^{(p^d-1)\cdot k})$, wobei $\frac{p^n-1}{p^d-1} = \sum_{i \in [0, \frac{n}{d}-1]} p^{id}$ ist. Daher zerfällt auch $X^{p^d} - X$ in $\mathbb{F}_{p^n}$ in verschiedene normierte Faktoren von Grad 1, d.h. es gibt p^d Elemente x in $\mathbb{F}_{p^n}$, die $x^{p^d} = x$ erfüllen.

Nach (2) kann es für jeden Teiler d von n höchstens einen Teilkörper $L \subseteq \mathbb{F}_{p^n}$ mit $|L| = p^d$ geben, da jedes $x \in L$ auch $x^{p^d} = x$ erfüllt, also $L \subseteq K_d$ gilt, und wegen $|L| = |K_d|$ also $L = K_d$ ist.

Sei Z ein Teilkörper von $\mathbb{F}_{64}$.

Es ist $6 = [\mathbb{F}_{64} : \mathbb{F}_2] = [\mathbb{F}_{64} : Z][Z : \mathbb{F}_2]$, d.h. $|Z| \in \{2, 2^2, 2^3, 2^6\} = \{2, 4, 8, 64\}$, und also $Z \in \{K_1, K_2, K_3, K_6\}$.

Somit hat $\mathbb{F}_{64}$ genau die 4 Teilkörper $\mathbf{K}_1, K_2, K_3, K_6$, wobei $|K_1| = 2$, $|K_2| = 4$, $|K_3| = 8$ und $|K_6| = 64$.

Aufgabe 51 Sei $n \in \mathbb{Z}_{\geqslant 1}$. Seien K und L Körper mit $|K| = |L| = p^n$ Elementen.

(1) Sei $a \in K$ mit $K = \mathbb{F}_p(a)$. Man zeige: Es gibt ein $b \in L$ mit

$$\mu_{b,\mathbb{F}_p}(X) = \mu_{a,\mathbb{F}_p}(X) \ .$$

(2) Sei $f(X) \in \mathbb{F}_p[X]$ normiert und irreduzibel von Grad n. Dann gibt es ein $b \in L$ mit

$$\mu_{b,\mathbb{F}_p}(X) = f(X) \ .$$

(3) Es ist

$$X^{p^n} - X = \prod_{\substack{f(X) \in \mathbb{F}_p[X] \\ \text{normiert und irreduzibel} \\ \deg(f(X)) | n}} f(X) \ .$$

Lösung zu Aufgabe 51:

(1) Nach Lemma 273 gibt es einen Körperisomorphismus $\alpha : K \xrightarrow{\sim} L$. Da $\alpha(\lambda \cdot a^k) = \lambda(\alpha(a))^k$ für $k \in [0, n]$, $\lambda \in \mathbb{F}_p$ ist, ist $\alpha(a) \in L$ eine Nullstelle des Minimalpolynoms $\mu_{a,\mathbb{F}_p}(X)$. Da $\mu_{a,\mathbb{F}_p}(X)$ normiert und irreduzibel ist, folgt

$$\mu_{\alpha(a),\mathbb{F}_p}(X) = \mu_{a,\mathbb{F}_p}(X) \ .$$

(2) Nach Lemma 196 ist $K := \mathbb{F}_p[X]/(f(X))$ ein Körper mit p^n Elementen, $f(X)$ das Minimalpolynom von $a := X + (f(X))$ und $K = \mathbb{F}_p(a)$. Nun folgt die Aussage mit (1).

(3) Es ist $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$ und daher

$$\mathrm{ggT}(X^{p^n} - X, (X^{p^n} - X)') = \mathrm{ggT}(X^{p^n} - X, -1) = 1 \ .$$

Nach Lemma 228(1) ist das Polynom $X^{p^n} - X$ quadratfrei in $\mathbb{F}_p[X]$.

Es genügt also zu zeigen, dass ein normiertes, irreduzibles Polynom $f(X) \in \mathbb{F}_p[X]$ mit $\deg(f(X)) = d$ das Polynom $X^{p^n} - X$ genau dann teilt, wenn d ein Teiler von n ist.

Zu $\Rightarrow$. Sei $f(X)$ ein irreduzibles, normiertes Polynom von Grad d, das $X^{p^n} - X$ teilt.

Es zerfällt $X^{p^n} - X \in \mathbb{F}_{p^n}[X]$ in verschiedene normierte Faktoren von Grad 1, also auch $f(X)$. Daher hat $f(X)$ eine Nullstelle in $\mathbb{F}_{p^n}$ und $Z := \mathbb{F}_p[X]/(f(X))$ ist ein Teilkörper von $\mathbb{F}_{p^n}$.

Nun ist, $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : Z][Z : \mathbb{F}_p] = [\mathbb{F}_{p^n} : Z] \cdot d$ nach dem Gradsatz, und also d ein Teiler von n.

Zu $\Leftarrow$. Nach (2) gibt es ein Element $b \in \mathbb{F}_{p^d}$ mit $f(X) = \mu_{b,\mathbb{F}_p}(X)$ und $\mathbb{F}_p(b) = \mathbb{F}_{p^d}$.

Jedes x in $\mathbb{F}_p(b)$ erfüllt $x^{p^d} = x$, also auch b. Da $f(X) = \mu_{b,\mathbb{F}_p}(X)$ ist und $X^{p^d} - X \in \mathbb{F}_p[X]$ liegt und b als Nullstelle hat, ist $f(X)$ ein Teiler $X^{p^d} - X$ vgl. Lemma 195.

Da d ein Teiler von n ist, gibt es ein $k \in \mathbb{Z}$ mit $n = k \cdot d$. Es ist $p^d - 1$ ein Teiler von $p^n - 1$, da $p^n - 1 = (p^d)^k - 1 = (p^d - 1)\left(\sum_{i \in [0,k-1]} p^{id}\right)$ ist.

Also hat $a := c^{\frac{(p^n-1)}{(p^d-1)}}$ Ordnung $|\langle a \rangle| = p^d - 1$ und alle Elemente $x \in \langle a \rangle$ erfüllen $x^{p^d-1} = 1$. D.h. das Polynom $X^{p^d} - X$ hat genau p^d Nullstellen. Jede Nullstelle von $X^{p^d} - X$ in $\mathbb{F}_{p^n}$ ist auch Nullstelle von $X^{p^n} - X$. Somit ist $X^{p^d} - X$ ein Teiler von $X^{p^n} - X$.

Alternativ: Man zeigt wie oben in Aufgabe 50(4), dass $X^{p^d} - X$ ein Teiler von $X^{p^n} - X$ ist.

Insgesamt ist $f(X)$ somit ein Teiler von $X^{p^n} - X$.

Aufgabe 52

(1) Man konstruiere einen Körperisomorphismus $\mathbb{F}_5(\gamma) \xrightarrow{\sim} \mathbb{F}_5(\tilde{\gamma})$, wobei $\gamma^2 = 2$ und $\tilde{\gamma}^2 = 3$ ist.

(2) Man konstruiere, unter Verwendung von zwei verschiedenen irreduziblen Polynomen, zwei Körper K und L mit $|K| = |L| = 9$. Man gebe einen Körperisomorphismus $K \xrightarrow{\sim} L$ an.

(3) Man bestimme für jedes irreduzible Polynom $f(X) \in \mathbb{F}_2[X]$ mit $\deg(f(X)) = 4$ ein Element $b \in \mathbb{F}_{16}$ mit $\mu_{b,\mathbb{F}_2}(X) = f(X)$.

(4) Man verifiziere durch direkte Rechnung, dass

$$X^{16} - X = \prod_{\substack{f(X)\in\mathbb{F}_2[X] \\ \text{normiert und irreduzibel} \\ \deg(f(X))|4}} f(X)$$

ist.

Lösung zu Aufgabe 52:

(1) Es hat $X^2 - 2$ keine Nullstelle in $\mathbb{F}_5$ und ist daher irreduzibel in $\mathbb{F}_5[X]$. Es ist $\mu_{\gamma,\mathbb{F}_5}(X) = X^2 - 2$. Wir suchen ein Element $c \in \mathbb{F}_5(\tilde{\gamma})$ mit $\mu_{\gamma,\mathbb{F}_5}(c) = c^2 - 2 = 0$.

Es ist $(1, \tilde{\gamma})$ eine $\mathbb{F}_5$-lineare Basis von $\mathbb{F}_5(\tilde{\gamma})$.

Die Bedingung $2 \stackrel{!}{=} (a_0 + a_1\tilde{\gamma})^2 = a_0^2 + 2a_0a_1\tilde{\gamma} + a_1^2 \cdot 3$ liefert $a_0a_1 = 0$ und $a_0^2 + 3a_1^2 = 2$ für $a_0, a_1 \in \mathbb{F}_5$. Ist $a_1 = 0$, dann ist $a_0^2 \stackrel{!}{=} 2$ unlösbar. Also ist $a_1 \neq 0$ und $a_0 \stackrel{!}{=} 0$. Wir können $a_1 = 2$ wählen. Dann ist für $c = 2\tilde{\gamma}$ die Bedingung $c^2 = 4 \cdot 3 = 2$ erfüllt.

Mit Lemma 202 erhalten wir den Körpermorphismus

$\alpha : \mathbb{F}_5(\gamma) \xrightarrow{\sim} \mathbb{F}_5(\tilde{\gamma}) : a_0 + a_1\gamma \mapsto a_0 + a_1 \cdot 2\tilde{\gamma}$ für $a_0, a_1 \in \mathbb{F}_5$. Als Körpermorphismus ist α injektiv. Da $|\mathbb{F}_5(\gamma)| = 25 = |\mathbb{F}_5(\tilde{\gamma})|$ ist, ist α auch surjektiv und daher ein Isomorphismus.

(2) Es haben z.B. $X^2 + 1$ und $X^2 + X + 2$ keine Nullstelle in $\mathbb{F}_3$ und sind daher irreduzibel in $\mathbb{F}_3[X]$. Sei $K = \mathbb{F}_3[X]/(X^2+1) = \mathbb{F}_3(\iota)$ mit $\iota := X+(X^2+1)$ und $L = \mathbb{F}_3[X]/(X^2+X+2) = \mathbb{F}_3(\tilde{\iota})$ mit $\tilde{\iota} := X + (X^2 + X + 2)$. Es ist $\iota^2 = -1$ und $\tilde{\iota}^2 = -\tilde{\iota} - 2 = 2\tilde{\iota} + 1$.

Wir suchen $c \in L$ mit $c^2 + 1 = 0$. Es ist $(1, \tilde{\iota})$ eine $\mathbb{F}_3$-lineare Basis von $\mathbb{F}_3(\tilde{\iota})$.

Die Bedingung $-1 = 2 \stackrel{!}{=} (a_0 + a_1\tilde{\iota})^2 = a_0^2 + 2a_0a_1\tilde{\iota} + a_1^2 \cdot (2\iota + 1)$ liefert $2a_0a_1 + 2a_1^2 = 0$ und $a_0^2 + a_1^2 = 2$ für $a_0, a_1 \in \mathbb{F}_3$. Ist $a_1 = 0$, dann ist $a_0^2 \stackrel{!}{=} 2$ unlösbar. Also ist $a_1 \neq 0$ und aus $2a_0 + 2a_1 \stackrel{!}{=} 0$ folgt $a_0 = -a_1$. Z.B. ist für $c = 1 - \tilde{\iota}$ die Bedingung $c^2 = 2$ erfüllt.

Mit Lemma 202 erhalten wir den Körpermorphismus

$$\alpha : K \xrightarrow{\sim} L : a_0 + a_1\iota \mapsto a_0 + a_1 \cdot (1 - \tilde{\iota})$$

für $a_0, a_1 \in \mathbb{F}_3$. Als Körpermorphismus ist α injektiv. Da $|K| = 9 = |L|$ ist, ist α auch surjektiv und daher ein Isomorphismus.

(3) Wir konstruieren $\mathbb{F}_{16}$ als $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$ und schreiben $\delta := X + (X^4 + X + 1)$. Es ist $\delta^4 = \delta + 1$.

Die Ordnung von δ ist ein Teiler von 15. Da $\delta^3 \neq 1$ ist und $\delta^5 = \delta^2 + \delta \neq 1$ ist, ist sie 15.

Es sind $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$ alle irreduziblen Polynome in $\mathbb{F}_2[X]$ von Grad 4, vgl. Beispiel 272.

Nach Konstruktion ist $\mu_{\delta,\mathbb{F}_2}(X) = X^4 + X + 1$.

Mit Hilfe des Frobenius-Endomorphismus ergibt sich $\mu_{\delta,\mathbb{F}_2}(X) = \mu_{\delta^2,\mathbb{F}_2}(X) = \mu_{\delta^4,\mathbb{F}_2}(X) = \mu_{\delta^8,\mathbb{F}_2}(X)$, denn z.B. ist $(\delta^2)^4 + \delta^2 + 1 = (\delta^4 + \delta + 1)^2 = 0$.

Es ist δ^3 Nullstelle von $X^4 + X^3 + X^2 + X + 1$, denn

$$\begin{aligned}(\delta^3)^4 + (\delta^3)^3 + (\delta^3)^2 + \delta^3 + 1 &= (\delta+1)^3 + (\delta+1)^2 \cdot \delta + (\delta+1)\delta^2 + \delta^3 + 1\\ &= (\delta+1)^2(\delta+1+\delta) + \delta^3 + \delta^2 + \delta^3 + 1\\ &= (\delta+1)^2 + \delta^2 + 1\\ &= \delta^2 + 1 + \delta^2 + 1\\ &= 0\ .\end{aligned}$$

Somit ist $\mu_{\delta^3,\mathbb{F}_2}(X) = X^4 + X^3 + X^2 + X + 1$.

Mit Hilfe des Frobenius-Endomorphismus ergibt sich $\mu_{\delta^3,\mathbb{F}_2}(X) = \mu_{\delta^6,\mathbb{F}_2}(X) = \mu_{\delta^{12},\mathbb{F}_2}(X) = \mu_{\delta^9,\mathbb{F}_2}(X)$.

Es ist $\delta^7 = \delta^4 \cdot \delta^3 = (\delta+1)\delta^3 = \delta^3 + \delta + 1$ Nullstelle von $X^4 + X^3 + 1$, denn

$$\begin{aligned}(\delta^7)^4 + (\delta^7)^3 + 1 &= \delta^{28} + \delta^{21} + 1\\ &= \delta^{13} + \delta^6 + 1\\ &= \delta(\delta+1)^3 + \delta^2(\delta+1) + 1\\ &= \delta(\delta+1)(\delta^2+1) + \delta^3 + \delta^2 + 1\\ &= \delta^4 + \delta^3 + \delta^2 + \delta + \delta^3 + \delta^2 + 1\\ &= \delta + 1 + \delta + 1\\ &= 0\ .\end{aligned}$$

Somit ist $\mu_{\delta^3+\delta+1,\mathbb{F}_2}(X) = X^4 + X^3 + 1$.

Mit Hilfe des Frobenius-Endomorphismus ergibt sich $\mu_{\delta^7,\mathbb{F}_2}(X) = \mu_{\delta^{14},\mathbb{F}_2}(X) = \mu_{\delta^{13},\mathbb{F}_2}(X) = \mu_{\delta^{11},\mathbb{F}_2}(X)$.

(4) Die Teiler von 4 sind $1, 2, 4$.

Nach Beispiel 272 gibt es in $\mathbb{F}_2[X]$ die irreduziblen Polynome $X, X+1$ von Grad 1, $X^2 + X + 1$ von Grad 2, sowie $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$ von Grad 4.

Es ergibt sich

$$\begin{aligned}&(X^4+X+1)\cdot(X^4+X^3+1)\cdot(X^4+X^3+X^2+X+1)\cdot(X^2+X+1)\cdot(X+1)\cdot X\\ =\ &(X^4+X+1)\cdot(X^4+X^3+1)\cdot(X^5+1)\cdot(X^2+X+1)\cdot X\\ =\ &(X^4+X+1)\cdot(X^4+X^3+1)\cdot(X^8+X^7+X^6+X^3+X^2+X)\\ =\ &(X^8+X^7+X^5+X^4+X^3+X+1)\cdot(X^8+X^7+X^6+X^3+X^2+X)\\ =\ &X^{16}+X^{15}+X^{14}+X^{11}+X^{10}+X^9\\ &+X^{15}+X^{14}+X^{13}+X^{10}+X^9+X^8\\ &+X^{13}+X^{12}+X^{11}+X^8+X^7+X^6\\ &+X^{12}+X^{11}+X^{10}+X^7+X^6+X^5\\ &+X^{11}+X^{10}+X^9+X^6+X^5+X^4\\ &+X^9+X^8+X^7+X^4+X^3+X^2\\ &+X^8+X^7+X^6+X^3+X^2+X\\ =\ &X^{16}+2\cdot X^{15}+2\cdot X^{14}+2\cdot X^{13}+2\cdot X^{12}+4\cdot X^{11}+4\cdot X^{10}+4\cdot X^9+4\cdot X^8+\\ &4\cdot X^7+4\cdot X^6+2\cdot X^5+2\cdot X^4+2\cdot X^3+2\cdot X^2+X\\ =\ &X^{16}-X\ .\end{aligned}$$